

### **Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

### **Listing of Claims:**

1. (Currently Amended) An arrangement for protection of end user personal profile data in a communication system including a number of end user stations and a number of service/information/content providers, or holding means holding end user personal profile data, the arrangement comprising:

an intermediary ~~An intermediate~~ proxy server supporting a first communication protocol for end user station communication;

a personal profile data protection server, for protecting end user personal profile data, supporting a second communication protocol for communication with the intermediary proxy server and a third communication protocol for communication with one of said service/information/content providers, said ~~personal profile data~~ protection server further comprises

an application programming interface (API) allowing service/information/content provider queries/interactions, and

storing means for storing of end user specific data and end user personal profile data, the ~~personal profile data~~ protection server having a protection certificate;

means for providing published certificates to the intermediary proxy server; and

~~wherein the intermediary proxy server comprising further comprises~~

means for verifying the authenticity ~~genuinity~~ of the protection certificate requested over said second communication protocol from the ~~personal profile~~ protection server against a published certificate and,

responsive to receipt of a verified genuine protection certificate of the ~~personal profile data~~ protection server, the service/information/content provider service/information content server requesting ~~can request~~, via the API, the end user personal profile data, which and ~~the in that personal profile data~~ is delivered according to end

user preferences or delivered ~~in such a manner that there is~~ having no association between the actual end user and the personal profile data of the end user.

2. (Previously Presented) The arrangement according to claim 1, wherein the first communications protocol is a secure protocol.

3.-4. (Canceled)

5. (Currently Amended) The arrangement according to claim 1, wherein the second communication protocol is a secure protocol.

6. (Canceled)

7. (Previously Presented) The arrangement according to claim 1, wherein the intermediary proxy server is a HTTP proxy.

8. (Previously Presented) The arrangement according to claim 1, wherein the intermediary proxy server comprises holding means for holding published certificates.

9. (Previously Presented) The arrangement according to claim 1, wherein the intermediary proxy server is in communication with external holding means holding published certificates.

10. (Canceled)

11. (Previously Presented) The arrangement according to claim 1, wherein the intermediary proxy server is located within an intranet or at the operator's premises.

12. (Previously Presented) The arrangement according to claim 1, wherein the intermediary proxy server comprises a functionality for establishing a security communication agreement with the protection server.

13. (Previously Presented) The arrangement according to claim 12, wherein the user preferences are stored in the end user station.

14. (Currently Amended) The arrangement according to claim 12, wherein the user preferences relating to privacy level are stored in the intermediary proxy server.

15. (Previously Presented) The arrangement according to claim 13, wherein the user preferences relating to privacy level are stored in separate fast access storing means after completion of the security communication agreement.

16. (Currently Amended) The arrangement according to claim 15, wherein the protection server comprises an API allowing service provider control of site and page policies, and in that if the end user privacy level is increased, data below the privacy level is deleted.

17. (Currently Amended) The arrangement according to claim 16, wherein the protection ~~proxy~~ server provides certificates, and preferably signatures upon request by said intermediary proxy server.

18.-19. (Canceled)

20. (Previously Presented) The arrangement according to claim 1, wherein the protection server storing means comprises at least three tables containing information about end user specific data, personal profile data information and statistical data respectively.

21. (Previously Presented) The arrangement according to claim 20, wherein the end user specific data and end user personal profile data is provided to the service provider in such a manner that the end user cannot be traced by the service provider.

22. (Currently Amended) The arrangement according to claim 21, wherein the protection ~~proxy~~ server comprises means for pseudonymizing statistical information and personal profile information by using a unique pseudo for each URL of the service provider that is requested.

23. (Currently Amended) A method for protection of end user personal profile data in a communication system with a number of end user stations and a number of service/information/content providers, the method comprising the steps of:

- registering a certificate for an end user personal profile a protection server for protecting end user personal profile data with a trusted third party,
- providing a request for the certificate from an intermediary proxy server in communication with an end user station using a first communication protocol, to the protection server over a second communication protocol,
- providing a response from the protection server to the intermediary server,
- verifying, in the intermediary proxy server that the certificate is genuine, thereby belonging to the respective protection server and is registered with the trusted third party,
- after confirmation that the protection server ~~[[/]]~~ certificate is genuine,
- allowing the service provider ~~having acquired the protection server~~ to retrieve end user data and personal profile data from the protection server according to policy setting and end user privacy level over an Application Programming Interface and a third communication protocol.

24. (Previously Presented) The method according to claim 23, further comprising the step of establishing an end user personal profile data security

agreement between the intermediary proxy server and the protection server (on behalf of the end user and the service provider).

25. (Currently Amended) The method according to claim 24, wherein the end user personal profile data security agreement comprises a P3P agreement.

26.-28. (Canceled).

29. (Currently Amended) The method according to claim 24 ~~[[23]]~~, wherein the end user preferences (privacy levels) are stored in the end user station or in the intermediary proxy server, and in that they can be separately stored after confirmation of the end user personal profile data security agreement.

30. (Previously Presented) The method according to claim 23, further comprising the steps of:

- providing an API at the protection server,
- using the API for queries to the protection servers from the service provider,
- providing responses over a third communication protocol to the service provider.

31. (Previously Presented) The method of claim 30, further comprising the step of storing data in a number of tables in the protection server relating to user specific data, end user personal profile data and statistical data.

32. (Previously Presented) The method of claim 31, further comprising the step of pseudonymizing statistical data and profile information such that end user personal data cannot be associated or tied to the actual end user.

33. (Currently Amended) The arrangement according to claim 1, wherein the intermediary intermediate proxy server is located within a personal environment of the end user.

34. (Currently Amended) The arrangement according to claim 1, wherein the intermediary intermediate proxy server is located within premises of the end user.

35. (Currently Amended) The arrangement according to claim 1, wherein the intermediary intermediate proxy server is located within an intranet utilized by the end user.